What is claimed is:

1. A broadcasting server system for protecting and managing digital broadcasting contents, comprising:

a control means for generating access control information and a control word based on subscriber information, the access control information including CAT, entitlement control message (ECM) and entitlement management message (EMM);

an additional data generation means for generating additional data including use control metadata, tool information metadata, and content purchase information metadata to protect and manage the digital broadcasting contents;

a watermarking means for receiving an identification of a broadcasting content, which is referred to as a content ID, and the use control metadata, and watermarking an audio/video (A/V) media signal by using the content ID and the use control metadata as watermarks, the use control metadata including copy control information (CCI), broadcasting flag (BF) and retention information (RI);

a media encoding means for compressing the watermarked A/V media signal;

an encrypting means for encrypting the compressed A/V media signal;

a multiplexing means for receiving and multiplexing the

compressed and encrypted A/V media signal to thereby output a media transport stream;

a re-multiplexing means for receiving and re-multiplexing the media transport stream, the additional data and the access control information to thereby output a re-multiplexed signal; and

a scrambling means for scrambling the re-multiplexed signal by using the control word.

2. The system as recited in claim 1, further comprising:

a purchase result management means for managing broadcasting content purchase result of a user; and

a monitoring result management means for managing broadcasting content monitoring result.

3. The system as recited in claim 1, wherein the content ID is abstracted and used for determining whether a content is an unlawful broadcasting content when the broadcasting content is distributed unlawfully, or the content ID is abstracted and used for determining whether a content that are broadcasted currently is authentic or not after monitoring.

4. The system as recited in claim 1, wherein the use control metadata include the CCI, the BF and the RI,

determines from the CCI whether a broadcasting content can be copied, identifies from the BF whether the content is a broadcasting content, and indicates in the RI how long the broadcasting content can be retained being stored in a hard disk of the receiver.

5. The system as recited in claim 4, wherein the tool information metadata include:

protection and management tool information on the protection and management tools used for protecting and managing the broadcasting content;

decrypting information needed for decrypting the broadcasting content to which the protection and management tools are applied, the decrypting information including watermarking information and encrypted transport stream information;

location information on locations to which the protection and management tools should be applied;

replaceable tool information on kinds of tools that can be replaced; and

tools.

6. The system as recited in claim 5, wherein the content purchase information metadata include purchase conditions used when the user purchases the broadcasting content, and a list of contents that can be purchased.

7. A method for operating a broadcasting server system for protecting and managing digital broadcasting contents, the method comprising the steps of:

a) generating access control information and a control word based on subscriber information, the access control information including CAT, entitlement control message (ECM) and entitlement management message (EMM);

b) generating additional data including use control metadata, tool information metadata and content purchase information metadata to protect and manage the digital broadcasting contents;

c) receiving an identification of a broadcasting content, which is referred to as a content ID, and the use control metadata and watermarking an audio/video (A/V) media signal by using the content ID and the use control metadata as watermarks, the use control metadata including copy control information (CCI), broadcasting flag (BF) and retention information (RI);

d) compressing the watermarked A/V media signal;

e) encrypting the compressed A/V media signal;

f) receiving and multiplexing the compressed and encrypted A/V media signal to thereby output a media transport stream;

g) receiving and re-multiplexing the media transport stream, the additional data and the access control information

to thereby output a re-multiplexed signal; and

h) scrambling the re-multiplexed signal by using the control word.

8. The method as recited in claim 7, further comprising a step of:

i) managing a broadcasting content purchase result of a user and managing a broadcasting content monitoring result.

9. The method as recited in claim 7, wherein the content ID is abstracted and used for determining whether a content is an unlawful broadcasting content when the broadcasting content is distributed unlawfully, or a content ID is abstracted and used for determining whether the content that are broadcasted currently is authentic or not after monitoring.

10. The method as recited in claim 7, wherein the use control metadata include the CCI, the BF and the RI, determines from the CCI whether a broadcasting content can be copied, identifies from the BF whether the content is a broadcasting content, and indicates in the RI how long the broadcasting content can be retained being stored in a hard disk of the receiver.

11. The method as recited in claim 10, wherein the tool

information metadata include:

protection and management tool information on the protection and management tools used for protecting and managing the broadcasting content;

decrypting information needed for decrypting the broadcasting content to which the protection and management tools are applied, the decrypting information including watermarking information and encrypted transport stream information;

location information on locations to which the protection and management tools should be applied;

replaceable tool information on kinds of tools that can be replaced; and

tools.

12. The method as recited in claim 11, wherein the content purchase information metadata include purchase conditions used when the user purchases the broadcasting content, and a list of contents that can be purchased.

13. A computer-readable recording medium for recording a program that implements a method for operating a broadcasting server system that protects and manages digital broadcasting contents, comprising the steps of:

a) generating access control information and a control word based on subscriber information, the access control

information including CAT, entitlement control message (ECM) and entitlement management message (EMM);

b) generating additional data including use control metadata, tool information metadata and content purchase information metadata to protect and manage the digital broadcasting contents;

c) receiving an identification of a broadcasting content, which is referred to as a content ID, and the use control metadata and watermarking an audio/video (A/V) media signal by using the content ID and the use control metadata as watermarks, the use control metadata including copy control information (CCI), broadcasting flag (BF) and retention information (RI);

d) compressing the watermarked A/V media signal;

e) encrypting the compressed A/V media signal;

f) receiving and multiplexing the compressed and encrypted A/V media signal to thereby output a media transport stream;

g) receiving and re-multiplexing the media transport stream, the additional data and the access control information to thereby output a re-multiplexed signal; and

h) scrambling the re-multiplexed signal by using the control word.